PODER JUDICIÁRIO
TRIBUNAL REGIONAL DO TRABALHO DA 8ª REGIÃO

RESOLUÇÃO TRT8 N.º 110, DE 7 DE DEZEMBRO DE 2023.

Estabelece a Política de Backup de Dados no âmbito do Tribunal Regional do Trabalho da 8ª Região.

O EGRÉGIO TRIBUNAL REGIONAL DO TRABALHO DA OITAVA REGIÃO, no uso de suas atribuições legais e regimentais e**,** em sessão ordinária hoje realizada, sob a Presidência do Excelentíssimo Desembargador MARCUS AUGUSTO LOSADA MAIA; presentes as Excelentíssimas Senhoras Desembargadoras e os Excelentíssimos Senhores Desembargadores IDA SELENE DUARTE SIROTHEAU CORREA BRAGA (Vice-Presidente), MARIA ZUILA LIMA DUTRA (Corregedora Regional), ROSITA DE NAZARÉ SIDRIM NASSAR, JOSÉ EDÍLSIMO ELIZIÁRIO BENTES, FRANCISCA OLIVEIRA FORMIGOSA, FRANCISCO SÉRGIO SILVA ROCHA, ALDA MARIA DE PINHO COUTO, GRAZIELA LEITE COLARES, LUIS JOSÉ DE JESUS RIBEIRO, WALTER ROBERTO PARO, RAIMUNDO ITAMAR LEMOS FERNANDES JÚNIOR, ANTONIO OLDEMAR COELHO DOS SANTOS, MARIA DE NAZARÉ MEDEIROS ROCHA e CARLOS RODRIGUES ZAHLOUTH JÚNIOR; assim como a Excelentíssima Senhora Procuradora Regional do Trabalho, Doutora REJANE DE BARROS MEIRELES ALVES; e

CONSIDERANDO a dependência crescente dos sistemas de informação nas atividades administrativas e judiciais do Tribunal Regional do Trabalho da 8ª Região;

CONSIDERANDO a criticidade dos dados armazenados em ambiente de produção, uma vez que a perda dos mesmos pode implicar na paralisação de atividades essenciais do Tribunal Regional do Trabalho da 8ª Região;

CONSIDERANDO a necessidade de regulamentar o procedimento de cópia de segurança dos dados armazenados nos servidores do Tribunal Regional do Trabalho da 8ª Região;

CONSIDERANDO o item 12.3 da norma ABNT NBR ISO/IEC 27.002:2022, que estabelece diretrizes para proteção contra perdas de dados através da utilização de cópias de segurança;

CONSIDERANDO a seção II do Guia Referencial de Segurança da Informação da Justiça do Trabalho de 2021, elaborado pelo Conselho Superior da Justiça do Trabalho, que estabelece diretrizes a serem seguidas pelos Regionais na elaboração de suas políticas e procedimentos de backup;

CONSIDERANDO a portaria PRESI n.º 838/2017, que define o que são sistemas essenciais e quais seus parâmetros de continuidade;

CONSIDERANDO o que consta nos autos do Processo Administrativo Eletrônico n.º 7856/2023;

CONSIDERANDO a deliberação do Egrégio Tribunal Pleno em sessão ordinária do dia 7 de dezembro de 2023,

RESOLVE:

Art. 1.º Estabelecer a Política de Backup de Dados no âmbito do Tribunal Regional do Trabalho da 8.ª Região, da qual são partes integrantes todas as normas, procedimentos complementares e afins editados pelo Tribunal.

CAPÍTULO I
DO ESCOPO

Art. 2.º A Política de Backup de Dados tem por objetivo estabelecer diretrizes para o processo de backup dos dados estruturados e não estruturados sob a guarda da Secretaria de Tecnologia da Informação e Comunicação (SETIN), visando garantir a segurança dos mesmos.

Art. 3.º As disposições desta resolução se aplicam a todos os dados administrados pela SETIN, hospedados na infraestrutura própria do Tribunal ou em nuvem contratada, bem como a todos os colaboradores do Tribunal ou parceiros/conveniados/contratados externos que tenham necessidade de acesso aos dados armazenados nessas infraestruturas.

CAPÍTULO II
DO GLOSSÁRIO DE TERMOS UTILIZADOS

Art. 4.º Para o disposto nesta resolução, considera-se, além dos termos definidos pelo Glossário de Segurança da Informação, conforme portaria PRESI 685/2023:

I - Ambiente de Produção: ambiente operacional instalado, configurado e mantido pela

SETIN, cuja finalidade é dar sustentação ao funcionamento dos sistemas e serviços de TIC do Tribunal;

II - Banco de Dados: estendendo o conceito apresentado no glossário, pode ser definido como um conjunto de dados estruturados inter-relacionados, armazenados de forma persistente em mídia física (disco rígido) e gerenciados por softwares específicos chamados Sistemas Gerenciadores de Banco de Dados (SGBDs).

III - Servidores de Aplicação: computadores, físicos ou virtuais, hospedados em uma rede distribuída e que fornecem o ambiente para a instalação e execução das aplicações.

CAPÍTULO III
DAS REFERÊNCIAS LEGAIS E NORMATIVAS

Art. 5.º A Política de Backup de Dados do Tribunal Regional do Trabalho da 8.ª Região observa os seguintes requisitos legais e normativos:

I - Norma ABNT NBR ISO/IEC 27002:2022 - Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação;

II - ISO/IEC 27017:2015 - Tecnologia da informação - Define diretrizes para os controles de segurança da informação aplicáveis ao provisionamento e uso de serviços de nuvem;
III - Guia Referencial de Segurança da Informação da Justiça do Trabalho de 2021, elaborado pelo Conselho Superior da Justiça do Trabalho;

IV - Política de Segurança da Informação do TRT8 (Resolução No 53/2023);

V - Política de Controle de Acesso aos Recursos de TIC do TRT8 (Portaria PRESI No 686/2023);

VI - Portaria PRESI N.º 838/2017.

CAPÍTULO IV
DOS BACKUPS DOS DADOS

Art. 6.º O backup dos dados consiste em realizar uma ou mais cópias de segurança, física(s) ou lógica(s), desses dados e/ou metadados necessários para sua preservação e restauração íntegra, em caso de necessidade.

§ 1.º Um backup deve ser utilizável em casos de: teste(s); auditoria(s); corrompimento físico ou lógico; indisponibilidade temporária ou permanente; e perda parcial ou total dos dados a partir do(s) qual(is) foi(ram) gerado(s).

§ 2.º Um backup pode ser gerado de forma manual ou automatizada, devendo-se sempre dar preferência à geração automatizada.

§ 3.º Um backup deve ser gerado, transportado e armazenado de forma segura, com controles físicos e lógicos compatíveis com os requisitos de confidencialidade, integridade e disponibilidade.

§ 4.º Os backups dos dados de produção dos serviços e sistemas de informação do Tribunal devem ser gerados periodicamente. Tal periodicidade será específica de cada tipo de dados, de forma a atender aos requisitos de segurança dos serviços e sistemas de informação que o acessam.

§ 5.º O procedimento de geração do backup deve ser realizado preferencialmente fora do horário de expediente do Tribunal, a fim de evitar que haja indisponibilidade dos serviços e sistemas do Tribunal.

§ 6.º O backup deve ser armazenado em disco(s) distinto(s), hospedado(s) em local distinto, daquele(s) no(s) qual(is) se encontram os dados originalmente copiados.

§ 7.º Caso não seja possível o armazenamento dos dados copiados em local fisicamente distinto do local dos dados originalmente copiados, a Coordenadoria de Infraestrutura Tecnológica deve dar ciência à Direção da SETIN.

CAPÍTULO V
DA AUTOMATIZAÇÃO DA GERAÇÃO DO BACKUP

Art. 7.º O processo de automatização da geração do backup deve ser dividido em três etapas: planejamento, implementação e controle.

§ 1.º O planejamento objetiva a identificação da melhor estratégia a ser utilizada.

§ 2.º A implementação objetiva, através do uso de mecanismos nativos e/ou ferramentas, automatizar a estratégia de backup escolhida na etapa de planejamento.

§ 3.º O controle objetiva assegurar a efetividade da estratégia de backup escolhida e

automatizada, no sentido de garantir a eficiência na recuperação/restauração dos backups gerados e a integridade dos mesmos.

CAPÍTULO VI
DAS ESTRATÉGIAS DE BACKUP

Art. 8.º Uma estratégia de backup consiste em um conjunto de definições e procedimentos de geração de backups, cujo objetivo é atender aos requisitos de negócio da organização.

§ 1.º Uma estratégia de backup deve ser, preferencialmente, específica para cada ativo de dados a ser copiado/salvo, podendo, em caso de possibilidade e conveniência, ser compartilhada.

§ 2.º A escolha da estratégia de backup mais adequada deve ser baseada nos seguintes critérios: criticidade dos dados armazenados para a organização; tamanho da massa de dados a ser copiada; recursos de armazenamento disponíveis para uso e seu custo; requisitos de segurança da organização; mecanismos/ferramentas disponíveis de geração de backup.

§ 3.º Uma estratégia de backup deve definir: o(s) dados a ser(em) copiado(s); os tipos de backups (físicos e/ou lógicos) gerados; a composição (completos, diferenciais e incrementais) dos backups gerados; o formato (plano, compactado ou criptografado) dos backups; o local de armazenamento (disco rígido e/ou fita magnética); a periodicidade de geração; a janela de execução (horário) da rotina de backup; e o período de retenção dos backups armazenados.

§ 4.º Para os dados de produção de todos os serviços e sistemas de informação em uso pelo Tribunal, a estratégia de backup adotada deve garantir a recuperação completa e íntegra dos mesmos até um momento, a ser definido em portaria da Presidência, anterior à ocorrência de um desastre.

§ 5.º Para os dados de produção dos serviços e sistemas essenciais do Tribunal, a estratégia de backup adotada deve garantir também que:

I - A recuperação dos dados armazenados em banco de dados possa ser realizada em um momento passado de até 30 (trinta) dias, de maneira que inconsistências lógicas nesse período possam ser identificadas e corrigidas;

II - Os dados expurgados (retirados fisicamente do banco de dados) sejam retidos pelo

prazo legal até o seu descarte definitivo. Na ausência de dispositivo legal que defina os critérios para expurgo e o período de retenção das informações expurgadas de processos administrativos/judiciais eletrônicos, serão considerados aqueles em uso pela Unidade de Gestão Documental do Tribunal para processos físicos;

III - A recuperação dos dados dos servidores de aplicação possa ser realizada em um momento passado de até 6 (seis) meses;

IV - A recuperação dos dados em servidor de arquivo possa ser realizada em um momento passado de até 2 (dois) anos;

V - A recuperação dos dados de logs dos sistemas e servidores de aplicação possa ser realizada em um momento passado de até 5 (cinco) anos.

CAPÍTULO VII
DA RECUPERAÇÃO/RESTAURAÇÃO DE BACKUPS

Art. 9.º Os tempos mínimo e máximo necessários para a recuperação/restauração do(s) backup(s) de cada ativo de dados, bem como a quantidade máxima aceitável de dados perdidos após a ocorrência de desastre, serão definidos em portaria da Presidência.

§ 1.º No caso dos dados dos serviços e sistemas essenciais, com o intuito de se minimizar o tempo de indisponibilidade, a tentativa de recuperação será realizada inicialmente a partir da promoção das réplicas (backups online) disponíveis. Somente em caso de falha no uso das réplicas é que serão recuperados/restaurados os backups offline disponíveis.

Art. 10. Testes de recuperação/restauração dos backups armazenados serão realizados periodicamente de forma amostral para assegurar que a confiabilidade dos meios de armazenamento, a integridade dos dados e o tempo de restauração das cópias estejam aderentes aos requisitos de continuidade de negócio definidos pelo Tribunal.

§ 1.º Anualmente, pelo menos 1 (um) teste de recuperação/restauração será realizado em cada um dos backups realizados nos serviços e sistemas.

§ 2.º Os backups serão restaurados em ambientes de teste distintos dos de produção, como forma de validação.

§ 3.º Um backup será considerado válido quando os dados originais puderem ser restaurados de forma íntegra;

§ 4.º Sempre que determinado procedimento de backup for alterado, o backup resultante deve ser testado.

§ 5.º Para cada teste realizado será gerado um relatório com os resultados obtidos, sendo este apresentado à direção, coordenadorias e demais partes interessadas da SETIN. Tal relatório fará parte das evidências de realização dos testes de continuidade da SETIN.

CAPÍTULO VIII
DAS RESPONSABILIDADES

Art. 11. Em relação aos backups dos dados do Tribunal, em ambiente on premise e na nuvem, é de responsabilidade da:

I - Divisão de Bancos de Dados (DIBAD) da SETIN, a automatização da geração e a realização periódica de testes de recuperação/restauração dos backups dos dados estruturados armazenados em bancos de dados;

II - Divisão de Data Center (DIDAC) da SETIN, a automatização da geração e a realização periódica de testes de recuperação/restauração dos backups dos servidores de aplicação e dos dados não estruturados, bem como a disponibilização dos meios de armazenamento necessários e de ferramenta de administração de backups.

Art. 12. Ao término da atividade de recuperação/restauração de um backup, CODES (Coordenadoria de Desenvolvimento de Sistemas) e/ou COSID (Coordenadoria de Sustentação e Inteligência de Dados) podem ser demandadas para validar os dados recuperados/restaurados.

Art. 13. Compete à Direção da SETIN solicitar ao Tribunal a disponibilização de infraestrutura e recursos adequados para a realização dos procedimentos de backups dos dados, com suporte da CODES/DIBAD e COINT/DIDAC.

CAPÍTULO IX
DA VIGÊNCIA

Art. 14. A Política de Backup de Dados do Tribunal deve ser revisada e atualizada periodicamente, no máximo, a cada 3 (três) anos, caso não ocorram eventos ou fatos

relevantes que exijam uma revisão imediata.

CAPÍTULO X
DAS DISPOSIÇÕES FINAIS

Art. 15. Quaisquer situações, relativas ao backup dos dados sob a guarda da SETIN, que porventura não foram previstas nesta política, deverão ser analisadas e decididas pelo Subcomitê Gestor de Tecnologia da Informação e Comunicação.

Art. 16. Fica revogada a Portaria PRESI n.º 147, de 15 de novembro de 2017.

Art. 17. Esta Resolução entra em vigor na data de sua publicação no Diário Eletrônico da Justiça do Trabalho.

MARCUS AUGUSTO LOSADA MAIA:886
Assinado de forma digital por MARCUS AUGUSTO LOSADA MAIA:886
Dados: 2023.12.11 14:27:03 -03'00'

MARCUS AUGUSTO LOSADA MAIA
Desembargador Presidente

FONTE: Divulgada no Diário Eletrônico da Justiça do Trabalho no dia 11 de dezembro de 2023 (segunda-feira) e considerada publicada no dia 12 de dezembro de 2023 (terça-feira).